[CSCO 3809]

UNITED STATES PATENT APPLICATION FOR AN OPTICAL TRANSPORT CONCENTRATOR AUDIT SYSTEM AND METHOD

Inventor:

JOE DEPAOLANTONIO

Prepared by:

WAGNER, MURABITO & HAO

Two North Market Street, Third Floor

San Jose, California 95113

(408) 938-9060

AN OPTICAL TRANSPORT CONCENTRATOR NETWORK AUDIT SYSTEM AND METHOD

FIELD OF THE INVENTION

This invention relates to the field of communication networks. In particular, the present invention relates to auditing an optical concentrator and presenting the results in a convenient user friendly manner.

BACKGROUND OF THE INVENTION

Electronic systems and circuits have made a significant contribution towards the advancement of modern society and are utilized in a number of applications to achieve advantageous results. Numerous electronic technologies such as digital computers, calculators, audio devices, video equipment, and telephone systems facilitate increased productivity and cost reduction in analyzing and communicating data, ideas and trends in most areas of business, science, education and entertainment. Often these advantageous results are achieved through the use of distributed resources that communicate with each other over a network. To obtain maximized performance from distributed resources it is usually critical for the communication devices to be maintained at performance levels that support rapid and reliable communication of information. Advances in the

performance capabilities of modern network communications are increasing the demand for efficient and network management and maintenance operations capable of addressing complicated troubleshooting problems.

Tremendous growth in communication traffic due to a seemingly insatiable desire for new services has led to an increased an demand for large bandwidth capabilities and is driving the rapid deployment of advance communication networks. New optical networking is one example of advanced technologies that can efficiently support the exponential growth of data traffic through high performance bandwidth capabilities. Bandwidth is the rate at which information is communicated over a network. To support greater bandwidth and communication speed, modern communications systems utilizing advanced communication technology require communication devices to operate properly. The communication devices included in advanced networks are often complicated and sophisticated devices and to ensure information is communicated reliably, the communication devices usually have to operate within relatively stringent performance parameters. For example, communications over an optical network typically involves complicated engineering principals beyond the grasp of an average user. The complexities of advanced devices increase the difficulty in understanding how they are configured and operate. Network management and maintenance techniques directed to examining the

operation of the communication devices are often very complicated and consume significant resources.

Due to the complicated nature of the devices included in an advanced communications network, the technicians performing the troubleshooting are usually required to be highly skilled and experienced technicians. It takes a significant number of years to become highly skilled and experienced in the design and operations of devices included in a single communication network architecture. Advanced communications network device maintenance and management operations typically involve complicated protocols with obscure precise codes that are syntax sensitive and produce obfuscated data results presented in complicated formats. Manual entry of the precise codes and reading of the obfuscated data often results in errors. Even if the codes are entered correctly and the data is read correctly, viable network management and maintenance requires accurate interpretation, thoughtful analysis and insightful recommendations. In addition to solving existing problems a network communication device is experiencing, it is even more advantageous to have information on potential problems so that preventive measures can be taken to avoid loss of bandwidth capabilities. It usually takes significant resource expenditure to obtain the expertise required to provide network maintenance that addresses existing and potential communication device problems.

Communications networks typically involve large numbers of devices and information is often communicated over a number of different architectures and platforms. Each architecture usually encompasses a variety of devices each with unique auditing scenarios. The vast number of different devices that are potentially involved in communicating data over a network dramatically increases the knowledge and expertise and exponentially increases the difficulty of managing and maintaining network communication devices. It is particularly troublesome and very expensive to perform management and maintenance audits of all the different communications devices that are typically included in a modern communications network.

Accordingly, what is required is a system and method that facilitates audits of network communication devices and presents results in a convenient and user friendly format.

SUMMARY

The present invention is a system and method that facilitates audits of network device performance and presents results in a convenient and user friendly format. The present invention network device audit system and method provides audits of communication devices included in a communications network. In one embodiment, the present invention provides a system and method for auditing the characteristics and operations of a optical network concentrator. The communication device audit system and method efficiently and accurately assists management and maintenance operations for advanced network communication devices and provides a valuable proactive resource for end users.

A present invention automated network communication device audit tool interacts with other communication devices in a network, analyzes the condition and performance of the other communication devices, and reports the results in a convenient format. The present invention network communication device audit tool system and method automates the arduous process of gathering, parsing, analyzing, and organizing information required to create network communication device audit reports. In one embodiment, the present invention utilizes backend intelligence to discover and analyze problems with network communication devices and provides recommendations for potential solutions or corrective courses of action. In

one exemplary implementation of the present invention, a communication network device audit report provides information in a plain descriptive manner that facilitates easy understanding of the capabilities and problems of a communication network device. The communication network device audit reports the information in a similar look and feel format for a variety of communication devices from different architectures and protocols. For example, a present invention automated network communication device audit system and method audits the performance of an optical transport concentrator and provides an audit report that facilitates management and maintenance.

DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a flow chart of an automated network communication device audit tool method, one embodiment of the present invention.

Figure 2A is a block diagram of communications network that includes a present invention automated network communication device audit tool.

Figure 2B is a block diagram of an automated network communication device audit tool, one embodiment of the present invention.

Figure 3 is a block diagram illustration of one embodiment of a present invention network communication device audit report.

Figure 4A is an illustration of an automated network communication device audit report executive summary section included in one embodiment of the present invention.

Figure 4B is an illustration of one exemplary implementation of an introduction to network device audit section included in one embodiment of the present invention.

Figure 4C is an illustration of a exemplary implementation of a present invention network audit data collection summary section.

Figure 4D is an illustration of one embodiment of a present invention network audit data collection graph section.

Figure 4E is an illustration of one exemplary implementation of network audit data collection graph section included in one embodiment of the present invention.

Figure 5 is an illustration of a net audit detail section of one embodiment of the present invention.

Figure 6 is an illustration of a subimpact area net audit detail summary table included in one embodiment of a present invention.

Figure 7A is an illustration of a network element table included in one embodiment of the present invention for an optical concentrator.

Figure 7B is an illustration of an exemplary present invention board table.

Figure 7C is an illustration of a bits and synchronization reference table included in one exemplary implementation of the present invention.

Figure 7D is an illustration of a network element protection table included in one embodiment of the present invention.

Figure 7E is an illustration of one embodiment of a present invention optical facilities protection table.

Figure 7F is an illustration of a cross connect table included in one embodiment of the present invention.

Figure 7G is an illustration of a present invention exemplary DS1 service parameters table.

Figure 7H is an illustration of a DS3 service parameters table included in one exemplary implementation of the present invention.

Figure 7I is an illustration of an optical service parameter table included in one embodiment of the present invention.

Figure 8A is an illustration of a network element field notice table included in one embodiment of the present invention.

Figure 8B is an illustration of an alarm status table included in one embodiment of the present invention.

Figure 9A is an illustration of electrical performance near end table included in one embodiment of the present invention.

Figure 9B is an illustration of one exemplary implementation of a present invention optical performance far end table.

Figure 9C is an illustration of one embodiment of a present invention optical performance table.

Figure 10A is an illustration of a capacity planning table included in one embodiment of the present invention.

Figure 10B is an illustration of one embodiment of a present invention network communication device audit task list.

Figure 10C is an illustration of one embodiment of a present invention device unreachable table.

Figure 11A is a block diagram illustration of exemplary commands, retrieved network element information and guidelines for interpreting the retrieved information included in one exemplary implementation of the present invention.

Figure 11B is a block diagram illustration of one embodiment of present invention exemplary commands, retrieved network element information and guidelines for interpreting the retrieved information.

Figure 11C is a block diagram illustration of a partially populated exemplary far end optical performance table utilizing the correlation provided by the index correlation information.

Figure 11D is a table of network audit commands utilized in one embodiment of the present invention to retrieve information from an optical concentrator.

Figure 11E is a tabular illustration of network rules utilized in one exemplary implementation of the present invention.

Figure 11F is a tabular illustration of network rules utilized in one exemplary implementation of the present invention.

Figure 12 is one exemplary implementation of a present invention network element field notice table with corrective advice.

Figure 13 is one exemplary implementation of a present invention table included in an appendix with information on commands, impact areas, polling frequency, rule information, potential causes of a problem and suggested corrective measures.

DETAILED DESCRIPTION

Reference will now be made in detail to the preferred embodiments of the invention, an automated network communication device audit system and method, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the preferred embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one ordinarily skilled in the art that the present invention may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the current invention.

The present invention is an automated network communication device audit system and method that facilitates efficient and effective network resource management and maintenance. A present invention automated network communication device audit tool interacts with other communication devices in a network, analyzes the condition and

performance of the other communication devices, and reports the results in a convenient format. The present invention utilizes a backend intelligence to discover and analyze problems with devices included in a communication network and to provide recommendations for potential solutions or corrective courses of action. In one exemplary implementation of the present invention, a communication network device audit report provides information in a plain descriptive manner that facilitates easy understanding of the communication device capabilities and problems the communication device is exhibiting. For example, a present invention automated network communication device audit system and method automatically performs an optical transport concentrator audit and provides an audit report that assists network communication device management and maintenance activities.

Figure 1 is a flow chart of automated network communication device audit tool method 100, one embodiment of the present invention. In one embodiment of the present invention, automated network communication device audit tool method 100 is implemented on a computer system. In one exemplary implementation of the present invention, communication device information such as configuration, performance and functionality information is audited. Automated network communication device audit tool method 100 automates the arduous process of gathering, parsing, analyzing, and organizing communication network device information. configuration, performance and functionality information

In step 110, network communication device information is gathered. In one embodiment of the present invention, information indicating the types of devices included in a network and their status is retrieved. In one embodiment of the present invention, automated network communication device audit tool method 100 performs a network communication device query process that automatically queries the communication devices included in a network to obtain information of the device characteristics and operation. In one exemplary implementation of the present invention, automated network communication device audit tool method 200 automatically constructs the queries by issuing protocol commands formatted in the appropriate syntax for the communication devices included in the network. Figure 11D is a table of network audit commands utilized in one embodiment of the present invention to retrieve information from an optical concentrator. The information is gathered at predetermined intervals in accordance with a polling frequency or upon a triggering event (e.g., return from a network shutdown, operator command, etc.)

In step 120 the gathered information is parsed. In one embodiment of the present invention, automated network communication device audit tool method 100 automatically performs a parsing process that identifies portions of information retrieved in step 110 and correlates it to a operation or characteristic of the device. In one embodiment, a present invention utilizes

an intelligent backend to parse the information. For example, the intelligent backend includes information correlating the format of retrieved information to configuration, performance and functionality characteristics of the network communications device. In one exemplary implementation of the present invention, the intelligent backend is capable of recognizing character strings included in the gathered information and associating the character strings with a communication device characteristic. For example, a present invention network communications device audit intelligent backend is capable of recognizing that the character string HWVER=A0 included in information gathered in response to a >RTRV_INV::SLOT_ALL:301;< command indicates the hardware version is A0.

In step 130, automated network communication device audit tool method 100 determines if additional information is required. In one embodiment of the present invention, automated network communication device audit tool method 100 utilizes an intelligent backend to examine the information gathered in step 110 and ascertains if more detailed or precise information is required to perform the audit. For example, sufficient information to populate network audit report tables associated with the type of communication device being audited. In one exemplary implementation, the present invention network communications device audit intelligent backend includes information that draws a correlation between gathered information and additional requisite information. For example based upon

some particular retrieved information (e.g., a type of card or slot included in a communication device such as an OC3 card) the intelligent backend requests additional information directed at that type of card (optical performance characteristics such as errored seconds of the OC3 card). If additional information is required, automated network communication device audit tool method 100 returns to step 110 and performs additional information gathering based upon the requirements indicated by the intelligent backend. If additional information is not requested automated network communication device audit tool method 100 proceeds to step 140.

In one embodiment of a present invention implemented on a network comprising optical concentrators, information associated with the optical concentrators is gathered. For example, once automated network communication device audit tool method 100 determines the identity of the optical concentrators it forwards an iterative series of increasingly detailed queries. For example, automated network communication device audit tool method 100 forward commands directed to asking what cards are in which slots, what hardware version each card is, what software version are the cards are running, and what is the status of each card (e.g., is it working, in backup mode, not on, etc.). For each DS1 card or OC card identified in an optical concentrator the present invention asks each port on the DS1 card are there any coding violations, are there any errored seconds, any severely errored seconds, and any severely error frames. The present invention is intelligent

enough to form queries for different types of cards. For example, for each DS3 card identified, the present invention asks each port on the DS3 card what is the line type, the line code and the circuit build out.

In step 140 the characteristics and operation of communication devices included in a network are analyzed. In one embodiment of the present invention, an automated network communication device audit analysis process is utilized to analyze the configuration, functionality and performance of communication devices included in a communication network. In one exemplary implementation of the present invention, an expert network communications device audit intelligent backend compares the parsed information to values included in an expert network audit database. The values in the expert network audit database include threshold parameters that indicate acceptable characteristics, performance and functionality. Automated network communication device audit tool method 100 identifies if gathered information is within the threshold parameters.

In step 150, network communication device audit information is reported in a convenient manner including identification of existing and potential problems. In one embodiment of the present invention, the network communication device audit information includes device configuration information, functionality information, performance level information, and identification of parameters that do not meet threshold

levels. In one embodiment of the present invention, the network communication device audit report has the same look and feel for a variety of communication devices across different architectures and is organized in a manner that facilitates network management and maintenance.

In one exemplary implementation of the present invention, a present network device exemplary audit network report presents information associated with different areas that impact network management operations. For example, assessment of the health of a communication device is presented from network management operations impact areas such as fault management, performance management, configuration management, and capacity management. The fault management section provides information on faults (e.g., field notices). The performance management section includes information on operational problems (e.g., errored seconds). The configuration management section includes information of the components included in a node of a network element (e.g., a card part number). The capacity management section provides information expansion potential (e.g., slots available for additional cards). In one embodiment of the present invention, the impact areas are further broken down into subimpact areas such as system, media, protocol and node. The system section includes information on the system (e.g., hardware version, software version, part serial numbers, etc.). The media section includes information on the state of the communication media coupled to a network element (e.g., is there packet

loss, severely errored seconds, etc.). The protocol section includes information on communication standards applicable to a network element (e.g., is traffic communicated in accordance with TCP/IP requirements, apple talk requirements, Ethernet requirements, etc.) The node section includes environmental information (e.g., is a processor hot).

In one exemplary implementation of a present invention, an optical concentrator net audit tool system and method utilizes a unique methodology to analyze the "health" of a network. The present invention net audit methodology determines the characteristics of devices (e.g., an optical concentrator) within a network, compares the results to a set of established net rules, and identifies net rule exception points (NREPS). In one embodiment of the present invention, the net rules comprise definitions of predefined thresholds for acceptable tolerances associated with different characteristics of the network, for example different acceptable tolerances for components included in an optical concentrator. In one embodiment of the present invention, the net rules provide a standard by which the readiness and stability of a node is measured. In one embodiment the points are used to identify problems and potential problems.

In one embodiment of the present invention, network communication device responses and problems are assigned to a category and NREPs are assigned according to each category. In one exemplary implementation of the

present invention, results obtained from communication devices are divided into either an acceptable category, a warning category or a critical category. Each category is associated with predetermined parameter thresholds. In one exemplary implementation in which the results include information on errored seconds associated with a communication device, errored seconds within an acceptable predetermined range (e.g., 500 Seconds to 700 Seconds) is associated with the acceptable category, a questionable predetermined range (e.g., 450 Seconds to 500 Seconds) is associated with a warning category and an unacceptable range (e.g., 0 Seconds to 450 Seconds) is associated with a critical category.

The warning and critical audit results appear within network communication device audit tables in a different manner than acceptable audit results. For example, a warning threshold exceptions are presented in a special font (e.g., bold font) and in a contrasting color (e.g., yellow) and critical threshold exceptions are displayed distinguishing font (e.g., bold) and different color (e.g., red). The warnings are indicative of possible or potential problematic areas that should be considered for further investigation or corrective action. In one embodiment of the present invention, the warning category has a net rule exception point value of 1 which is assigned a device parameter (e.g., an optical concentrator laser power value) that is within the warning threshold ranges for the device parameter. Critical thresholds indicate a condition that requires prompt attention and corrective action. In

one embodiment of the present invention, the critical category has a net rule exception point value of 1,000 which is assigned a device parameter (e.g., an optical concentrator laser power value) that is within the critical threshold ranges for the device parameter.

Figure 2A is a block diagram of communications network 200. In one embodiment of the present invention, automated network communication device audit tool method 100 is implemented in communications network 200. Communications network 200 comprises network communication device audit tool system 250, dense wave division multiplexer (DWDM) 201 and 202, optical concentrators 210, 211, 121 and 217, routers 231, 240 and 287, cellular station 215, cellular device (e.g., phone, handheld computer, etc.) 299, microwave transceiver 281, internet 270, servers 285, 232, and 233, personal computers 235, 237, 239, 241, 271, 282, 283, 284, 288 and 289, and miscellaneous communication equipment 275 and 277. The components of communications network 200 communicate with each other over a variety of architectures utilizing numerous communication protocols. One exemplary implementation of communications network 200 utilizes Fiber Distributed Data Interface (FDDI), Dynamic Packet Transport (DPT), Packet Over Sonet (POS), Asynchronous Transfer Mode (ATM), Ethernet, token ring, Transmission Control Protocol/Internet Protocol (TCP/IP), plain old telephone system (POTS), Cable, Digital Subscriber Line (DSL), etc. Network

communication device audit tool system 250 audits the components of communications network 200.

The components of communications network 200 comprise network elements including nodes. For example, optical concentrator 210 has a chassis, a power supply and a mother board. The mother board comprises a plurality of printed circuit board (PCB) slots and busses between the slots. One slot includes a system board that comprises a processor and memory. The other slots include line cards such as a DS1 card, DS3 card, OC3 card, OC12 card, OC 48 card and OC192 card. Each of the line cards includes one or more ports. In one embodiment of the present invention, optical concentrators 210 provides cross connection between the facilities (e.g., line slots) with the ability to aggregate ("concentrate") communications from a number of electrical communication lines (e.g., DS ports) to an optical communication line (e.g., a OC port).

Figure 2B is a block diagram of automated network communication device audit tool 250, one embodiment of the present invention. In general, automated network communication device audit tool 250 comprises a bus 257, a central processor 251, a random access memory 252, a read only memory 253, a data storage device 254, a display device 255, an alphanumeric input device 256, a cursor control device 257 and a printer 258. Bus 257 is coupled to central processor 251, random access memory 252, read only memory 253, data

storage device 254, display device 255, alphanumeric input device 256, cursor control device 257 and printer 258.

The components of automated network communication device audit tool 250 cooperatively operate to perform their designated functions. Central processor 251 processes information and instructions including instructions associated with automated network communication device audit method 100. Random access memory 252 stores information and instructions for the central processor 251. Read only memory 253 stores static information and instructions for the processor 251. Data storage device 204 stores information and instructions (e.g., such as a magnetic or optical disk and disk drive). Display device 255 displays information to a computer user. Alphanumeric input device 256 includes alphanumeric and function keys for communicating information and command selections to the central processor 251. Cursor control device 257 communicates user input information and command selections to the central processor 251. Printer 258 prints documents in accordance with directions from central processor 251. Bus 257 is a path for communicating information. In one embodiment of the present invention, automated network communication device audit tool 250 also operates as an automated network communication audit intelligent backend.

The components of automated network communication device audit tool 250 comprise a variety of interchangeable embodiments. For example, the display device 255 of Figure 2B may be a liquid crystal device, cathode ray tube, or other display device suitable for creating graphic images and alphanumeric characters recognizable to the user. It is also to be appreciated that there are many implementations of cursor control device 257, including a trackball, mouse, joystick or a number of other specially adapted cursor directing devices for providing input to direct and/or activate the cursor. In one embodiment of automated transaction information management server 250, keys on alphanumeric input device 255 are also capable of signaling movement of a given direction or manner of displacement. For example, the cursor may be directed and/or activated via input from the keyboard of alphanumeric input device 255 using special keys and key sequence commands. Cursor control device 257 of automated transaction information management server 250 allows a computer user to dynamically signal the two dimensional movement of a cursor or visible symbol (pointer) on a display screen of the display device 255. Alternatively alphanumeric input device 255 allows the user to create graphic images and alphanumeric characters on a display screen of the display device 255.

Automated network communication device audit tool system 250 is a platform the performs automated network communication device audit tool method 100 and produces communication network device audit report 300 in

one embodiment of the present invention. Figure 3 is a block diagram illustration of one embodiment of network communication device audit report 300. Audit report 300 includes an executive summary section 310, net audit detail section 320, net audit task list section 330 and appendix section 340. Executive summary section 310 includes an executive summary that provides an overview of the "health and stability" of a communications device and results of the audit. Net audit detail section 320 includes audit detail tables that provide detailed information in a convenient user friendly format. In one embodiment of the present invention the net audit detail section is organized by type of network device and includes identification on a node by node basis of device values, expectations, and net rule exception points. Net audit task list section 330 includes a list that provides a hierarchical presentation of network device problems and potential problems in order of adverse impact on the reliability of a communication network. In one exemplary implementation of the present invention, the network audit task list provides a convenient summary of network rule exceptions on a node by node basis and suggested order of addressing problems. Appendix section 340 provides additional helpful information for interpreting the audit report.

Figure 4A is an illustration of automated network communication device audit report executive summary section 400 included in one embodiment of the present invention. Network audit report executive

summary section 400 comprises introduction to network device audit section 410, network audit data collection summary section 420, network audit data collection graph section 430, and network audit NREP summary section 440. Introduction to network device audit section 410 provides an introduction to the network device audit including a brief description of the device the audit is directed to (e.g., an optical concentrator) and the function of the device within the network. Figure 4B is an illustration of one exemplary implementation of introduction to network device audit section 410. Network audit data collection summary section 420 provides a convenient tabular formulation of the time the audit report covers and the number of unreachable nodes that are not analyzed by the audit. Figure 4C is an illustration of one exemplary implementation of network audit data collection summary section 420. Network audit data collection graph section 430 provides a graphical representation of the network audit data collection. For example, network audit data collection graph section includes a graph of warning or critical indication over time or a highest traffic analysis graph that indicated the top ten communication devices with highest aggregate bytes , or the sum of total transmit and received octects. Figure 4D is an illustration of one exemplary implementation of network audit data collection graph section 430. The net audit NREP summary includes an indication of the net audit health of a network communication device and an indication of the networks capabilities and performance.

Network audit NREP summary section 440 provides a quick reference summary of the NREP indications.

Figure 4E is an illustration of one exemplary implementation of network audit NREP summary section 440 comprising NREP category table 471, network audit health section 472, NREP summary table 473, NREP's ratio by category graph, network audit notes section 475, and NREP node correlation table 477. NREP category table 471 identifies and defines NREP categories and provides an indication of the NREPs assigned to each NREP category. Network audit health section 472 provides a convenient overall network audit health indicator. In one exemplary implementation of the present invention, the convenient overall network audit health indicator is a percentage indication equation such as (100-(total NREPs/total possible NREPs)100). NREP summary table 473 provides a convenient tabular summary of the total NREPs in each NREP category and total NREPs for the network. NREP's ratio by category graph includes a graphical representation of the NREPs by category. Network audit notes section 475 includes notes associated with the network audit. NREP node correlation table 477 includes a correlation of the NREPs to impact areas.

Figure 5 is an illustration of net audit detail section 500, one embodiment of a present invention net audit detail section. The net audit detail section provides information in convenient and efficient manner. Net

audit detail section 500 comprises net audit detail impact sections and subsections. Each of the net audit detail impact sections comprises information associated with a network impact area arranged in subimpact categories. In one exemplary implementation of the present invention, net audit detail section 500 comprises impact sections such as a configuration management section 510, a fault management section 520, a performance management section 530, and a capacity management section 540. Information in each of the impact sections is arranged according to subimpact areas such as system, media, node, and protocol.

In one embodiment of the present invention, a net audit detail section also includes a subimpact area net audit detail summary table. Figure 6 is an illustration of subimpact area net audit detail summary table 600 included in one embodiment of a present invention. Subimpact area net audit detail summary table 600 comprises a tabular listing of net rule exception points by node and impact area. This format of subimpact area net audit detail summary table 600 provides a quick and accurate overview of problems and potential problems associated with a subimpact area broken down by nodes included in the network element. In one exemplary implementation of the present invention, a subimpact area net audit detail summary table 600 is provided for each subimpact area (e.g., system, media, protocol, node, etc.).

Figure 7A is an illustration of a network element table 710 included in one embodiment of the present invention for an optical concentrator. In one exemplary implementation of the present invention, network element table 710 is included in configuration management section 510 system subsection 511. Network element table 710 lists the elements (e.g., optical concentrators) included in a network and the associated internet protocol (IP) address, node identification (ID), synchronous transmission mode (STM), and timing mode for each network element.

Figure 7B is an illustration of board table 720 included in one embodiment of the present invention. In one exemplary implementation of the present invention board table 720 is included in configuration management section 510 system subsection 511. The board table lists printed circuit boards (PCBs) included in a network element, the slot number occupied by the PCBs , the part numbers of the PCBs, the serial numbers, the hardware versions, firmware versions and the status of each PCB.

Figure 7C is an illustration of a bits and synchronization reference table 730 included in one embodiment of the present invention. Bits and synchronization reference table 730 is included in configuration management section 510 protocol subsection 513 in one exemplary implementation of the present invention. The bits and synchronization table lists the configuration settings for a network element.

Figure 7D is an illustration of a network element protection table 740 included in one embodiment of the present invention. Network element protection table 740 is included in configuration management section 510 protocol subsection 513 in one exemplary implementation of the present invention. The network element protection table 740 lists a protection scheme that is configured on a network element.

Figure 7E is an illustration of a optical facilities protection table 750 included in one embodiment of the present invention. Optical facilities protection table 750 is included in configuration management section 510 protocol subsection 513 in one exemplary implementation of the present invention. The optical facilities protection table 750 lists an optical service protection scheme that is configured on a network element.

Figure 7F is an illustration of a cross connect table 760 included in one embodiment of the present invention. Cross connect table 760 is included in configuration management section 510 protocol subsection 513 in one exemplary implementation of the present invention. The cross connect table displays the cross connects configured on the network element.

Figure 7G is an illustration of DS1 service parameters table 770 included in one embodiment of the present invention. DS3 service

parameters table 770 is included in configuration management section 510 media subsection 512 in one exemplary implementation of the present invention. The DS1 parameters table lists configuration and fault information for a DS1 facility (e.g., a DS1 slot) configured within a network element.

Figure 7H is an illustration of DS3 service parameters table 780 included in one embodiment of the present invention. DS3 service parameters table 780 is included in configuration management section 510 media subsection 512 in one exemplary implementation of the present invention. The DS3 service parameters table lists configuration and fault information for a DS3 facility (e.g., DS3 slot) configured within a network element.

Figure 7I is an illustration of optical service parameter table 790 included in one embodiment of the present invention. Optical service parameter table 790 is included in configuration management section 510 media subsection 512 in one exemplary implementation of the present invention. The optical services parameters table lists configuration and fault information an optical facility configured within the network element.

Figure 8A is an illustration of network element field notice table 810 included in one embodiment of the present invention. Network element

field notice table 810 is included in fault management section 520 media subsection 522 in one embodiment of the present invention. Network element field notice table 810 lists known product field notices know to possibly result in service interruptions. In one exemplary implementation of the present invention, network element field notice table 810 provides an indication that the field notice problems should be corrected immediately.

Figure 8B is an illustration of alarm status table 820 included in one embodiment of the present invention. Alarm status table 820 is included in fault management section 520 media subsection 522 in one exemplary implementation of the present invention. Alarm status table 820 lists network element alarms.

Figure 9A is an illustration of electrical performance table near end 910 included in one embodiment of the present invention. Electrical performance table far end 910 is included in performance management section 530 protocol subsection 533 in one exemplary implementation of the present invention. The electrical performance table lists performance and fault information for all the electrical facilitates configures within the network element when referenced from the near end.

Figure 9B is an illustration of optical performance table far end 920 included in one embodiment of the present invention. Optical performance

table far end 930 is included in performance management section 530 protocol subsection 533 in one exemplary implementation of the present invention. The optical performance table lists performance and fault information for all the optical facilitates configures within the network element when referenced from the near end.

Figure 9C is an illustration of optical performance table 930 included in one embodiment of the present invention. Optical performance table 930 is included in performance management section 530 system subsection 531 in one exemplary implementation of the present invention. The optical performance table lists performance and fault information for all the optical facilitates (e.g., OS) configured within the network element when referenced from the far end.

Figure 10A is an illustration of a capacity planning table 1010 included in one embodiment of the present invention. Capacity planning table 1010 is included in configuration management section 540 system subsection 511 in one exemplary implementation of the present invention. The capacity planning table displays the current configuration and slot position of cards in the network element and the availability of slots for future expansion.

A present invention net audit task list section (e.g., net audit task list section 330) provides guidance on a corrective plan of action for problems

with network communication devices. In one embodiment of the present invention, a network communication device audit task list provides network specific information system by system that assists implements of recommended corrective measures. Figure 10B is an illustration of network communication device audit task list 1020, one embodiment of a present invention network communication device audit task list. Network communication device audit task list 1020 lists the "worst" ranking audited network communication device nodes at the top of the list in which ranks are based on the assigned NREPS to each node. In one exemplary implementation, the net audit task list is utilized to easily reference information about the "bad" systems as well as comments, corrective advice and relevant appendix information.

An appendix section of the present invention (e.g., appendix section 340) provides additional helpful information for interpreting the audit report and understanding a network element. In one embodiment of the present invention includes a network advice section, a supporting reference section, and a device unreachable section. The network advice section provides details on the NREPs, values and exceptions. The supporting reference section includes information that assist interpretation of the terms utilized in the network audit report. In one exemplary implementation of the present invention provides a glossary and definition of acronyms utilized in the network audit report. The device unreachable section provides identification

of devices not reached during the audit process by the present invention. Figure 10C is an illustration of device unreachable table 1030, one embodiment of a present invention device unreachable table. In one exemplary implementation device unreachable table 1030 includes information explaining potential reasons for the inability to interact with a network communication device.

A present invention automated network communication device audit tool system and method automates the arduous process of gathering, parsing, analyzing, and organizing information required to create the net audit detail section reports. For example, automated network communication device audit tool system and method 200 automatically performs the tasks required to create concentrator optical performance near end table 920, such as formulation of commands compliant with precise syntax requirements, interpretation of convoluted retrieved information, identification of problems and reorganization of information for reporting in a convenient user friendly format. Figure 11A and 11B are block diagram illustrations of exemplary commands, retrieved network element information and guidelines for interpreting the retrieved information in one exemplary implementation of the present invention.

The command 1101 in Figure 11A and the command 1111 in Figure 11B for gathering network communication device information are

automatically configured by one embodiment of the present invention in the appropriate syntax format for an optical concentrator. For example, a present invention network audit system and method issues a command to retrieve inventory information on each slot included in an optical concentrator (e.g., command 1101 in Figure 11A). Figure 11D is a tabular compilation of commands utilized to obtain information from an optical concentrator in one exemplary implementation of the present invention. The italicized variables in the commands shown in Figure 11D are an indication of variables associated with particular network communication devices that the present invention automatically configures in the appropriate syntax. The present invention receives information in response to the commands (e.g., the retrieve command 1101 or retrieve optical performance of an OC48 command 1111) and correlates the information to the cells in the near end optical performance table 920 according to the guidelines shown in correlation sections 1103 and 1113 of Figure 11A and Figure 11B respectively.

In one embodiment, the present invention receives information in response to a command (e.g., retrieve command 1101) and performs a parsing process by establishing boundaries for portions of the received information. The boundaries are utilized to define information associated with a characteristic of a network element (e.g. configuration, performance or functionality information). For example, the characteristics are related to a column in a network audit table such as near end optical performance table

920. In one exemplary implementation, the present invention utilizes an intelligent backend expert system and parsing code software instructions to establish the boundaries and correlate the retrieved information to the boundaries. For example, the backend intelligent system includes information on the number of bits associated with a characteristic, counts over that number of bits and correlates those bits with the category and/or the backend intelligent system is capable of recognizing a character (e.g., a comma or semicolon, etc.) or character string (e.g., HWVER=A0) included in the gathered information and correlating the character strings with a characteristic.

Figure 11A and Figure 11B are shown so that the parsing of retrieved information may be more easily understood. The index identifiers included in section 1107 (which are a the same as those shown in index number column 1104) are not included in the retrieved information, they are merely shown to illustrate the automated correlation of the retrieved information to cell in near end optical performance table 920. Figure 11A index correlation section 903 and Figure 11B index correlation section 913 show a tabular representation of index correlation utilized to make correlations between information received from a network element (e.g., section 1109) and presentation of the information in a network audit detail table. For example, the field names shown in column 1105 correspond to the column headings in column in near end optical performance table 920.

Figure 11C is a block diagram illustration of a partially populated exemplary far end optical performance table. Please note that the information shown in row 1131 does not appear in the actual far end optical performance table, it is shown in figure 11C so as to provide an indication of the parsing relationship of the information shown in row 1132 to the information received from the network elements (e.g., section 1109). The information shown in row 1133 does not appear in the actual far end optical performance table, it is shown in figure 11C so as to provide an indication of NREP application to the information shown in row 1132. Figure 11E and Figure 11F are a tabular illustration of network rules utilized in one exemplary implementation of the present invention. In one exemplary implementation of the present invention, relevant network rules and/or corrective advice is provided below the network communication device audit tables comprising indications of warning or critical problems.

In one embodiment of the present information corrective advice is included in a network communication device audit table. In one exemplary implementation of the present invention, the corrective advice includes identification of potential causes of a problem and suggested remedial course of action. The identification of potential problems and suggested remedial courses permits a user to leverage the significant communication network device expertise accumulated and stored by a present invention automated

network communication device audit tool system and method. In one exemplary implementation, the information provides a user with insightful assistance and information that took many hours of trouble shooting a wide variety of communications in a number of environments subject to common and extraordinary operating constraints and performance levels. In one embodiment, an automated network communication device audit tool system and method tracks indications of problems with a communication device and a course of action that corrected the problem. When those indications appear again associated with the communication device, a automated network communication device audit tool system and method suggests it may be the same type of problem and a similar course of corrective action. In one embodiment of the present invention, potential problems and corrective courses of action are listed in a manner indicating the most likely cause of the problem and the course of action most likely to correct the problem.

The identification of problems and suggested courses of action cover a wide variety of communications devices and operating scenarios. In one exemplary implementation of the present invention, identification of a problem associated with a coding violation indication on an optical concentrator includes an indication that causes of coding violations can be noise, electrical or mechanical failures due to either circuit issues or with the linecard itself. If multiple lines from the same card exhibit the same

symptoms the problem could be linecard related. Individual instances could be circuit specific. To help isolate the problem further suggested testing includes as BIT Error Rate tests, mapping and demapping tests, payload pointer investigation, and embedded overhead or line interface testing. Figure 12 is one exemplary implementation of a network element field notice table (e.g., network element field notice table 810) with corrective advice. Figure 13 is one exemplary implementation of a present invention table included in a appendix with information on commands, impact areas, polling frequency, rule information, potential causes of a problem and suggested corrective measures.

The amount of information that is required to be parsed to provide the optical performance table far end table is quite significant. The retrieved information shown in section 902 of figure 9A covers one node of one network element, and in a typical network there are multiple nodes and network elements. The retrieved information shown in section 912 of figure 9B covers one slot of one node, and as indicated in Figure 9A there are typically multiple slots for each node. The number of lines of retrieved information that is shifted through, parsed and analyzed to provide optical performance table far end table is exponentially greater. To manually produce audit network tables an optical concentrator requires significant resources and is subject to numerous error. For example, the amount of syntax sensitive code that is transmitted and received is highly susceptible to manual entry

and interrelation errors. However, the present invention automates the process and reduces the susceptibility to manual entry and interrelation errors.

Thus, the present invention is a system and method that facilitates audits of network device performance and presents results in a convenient and user friendly format. A present invention network communication device audit tool system and method assists efficient and network management and maintenance operations capable of addressing complicated troubleshooting problems in advanced communication networks. The network communication device audit tool system and method provides reduction in the resources required to examine the operation of communication devices and identify when a communication device is not operating within relatively stringent performance parameters, indicate potential causes of the problem and suggest appropriate courses of action. The information is presented in a user friendly manner with a consistent look and feel for a variety of communication network device audits. The network communication device audit tool system and method aids maintenance and management operations involving complicated protocols with obscure precise codes that are syntax sensitive and produce obfuscated data results presented in complicated formats while promoting accurate interpretation, thoughtful analysis and insightful recommendations.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.